KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: G06F 13/00

(21) Application No.: 10-1997-0072765 (11) Publication No.: 10-1999-0053174

(22) Application Date: December 23, 1997 (43) Publication Date: July 15, 1999

(71) Applicant: Electronics and Telecommunications Research Institute

(72) Inventor(s): Yoo, Dae-hyun

Lee, Kyung-hyun

Shin- Sangwook

(54) Title of the Invention:

Method of Checking Data Integrity Using Hash Function

Abstract:

The present invention relates to a method of checking the integrity of data using a hash function.

The hash function maps arbitrary-length messages to short and fixed-length messages, and is used to check the integrity of data, configure a message-authentication code, and augment the efficiency of digital signatures. Configuring an algorithm that executes efficiently and has robust encryption characteristics is difficult. The present invention proposes performing a message extension that generates an additional 8 message words on an input message word, and uses a Boolean function that has robust encryption characteristics and a variable message-dependent rotation mechanism in which rotation operations in each step are dependent on the input message, thereby configuring an efficient hash function with robust encryption characteristics. Accordingly, a hash value that corresponds to the data is calculated when a data file is stored, and is transmitted along with the data in order to check the integrity of data; that is, to assure that the data has not been changed between creation and reception.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 13/00

(11) 공개번호 특1999-0053174
(43) 공개일자 1999년07월15일

(21) 출원번호 10-1997-0072765
(22) 출원일자 1997년12월23일

(71) 출원인 한국전자통신연구원 정선종
대전광역시 유성구 가정동 161번지
(72) 발명자 류대현
대전광역시 유성구 어은동 한빛 아파트 129동 1401호
이경현
부산광역시 해운대구 좌동 코오롱 아파트 107동 1701호
신상욱
부산광역시 해운대구 재송동 시영아파트 11-206호
(74) 대리인 신영무, 최승민

심사청구 : 있음

(54) 해쉬함수를 이용한 정보의 무결성 확인방법

요약

본 발명은 해쉬함수를 이용한 정보의 무결성 확인방법에 관한 것으로, 특히 정보 보호 분야에서 빈번하게 사용되는 중요한 암호 기술 중의 하나인 해쉬함수를 이용한 정보의 무결성 확인방법에 관한 것이다.

해쉬 함수는 임의의 길이 메시지를 고정된 짧은 길이로 사상시키는 함수로 중요정보의 무결성 확인과 메시지 인증코드의 구성, 디지털 서명의 효율성 증대를 위한 목적으로 사용된다. 알고리즘이 수행 속도면에서 효율적이어야 한다. 실제 암호적으로 안전하고 효율적인 해쉬 함수의 구성은 매우 어려운 문제이다. 따라서, 본 발명은 입력 메시지 워드로부터 추가로 8개의 메시지 워드를 생성하는 메시지 확장을 사용하고, 암호적으로 강한 성질들을 만족하는 부울 함수와 각 단계 연산에서 사용되는 로테이션 연산을 입력 메시지에 의존하는 가변적인 메시지-의존 로테이션(Message-dependent Rotation)을 사용하여 암호적으로 안전하고 효율적인 해쉬함수를 구성한다. 그 결과 정보의 전송시 그 정보에 대한 해쉬 값을 함께 전송함으로써 전송도중에 발생할 수 있는 제 3 자에 의한 정보의 수정 및 삽입 등의 문제에 대해 정보의 무결성을 확인할 수 있고, 데이터 파일의 저장시에 파일에 대한 해쉬 값을 계산해 둠으로서 중요 데이터에 대한 무결성을 확인할 수 있다.

대표도

도3

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 해쉬 함수의 전체 구조 블록도.

도 2는 본 발명에 따른 해쉬 함수의 압축 함수의 블록도.

도 3은 본 발명에 따른 해쉬 함수의 단계 연산의 블록도.

도 4는 본 발명에 따른 해쉬 함수에 대한 동작 흐름도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 해쉬함수를 이용한 정보의 무결성 확인방법에 관한 것으로, 특히 해쉬함수의 각 단계 연산에 암호학적으로 강한 성질들을 만족하는 부울 함수와 입력 메시지에 의존하는 메시지-의존 로테이션(Message-Dependent Rotation)을 사용하여 해쉬함수의 안전성을 향상시키는 것이다.

일반적으로, 해쉬 함수는 임의의 유한 길이 비트스트링을 고정된 길이의 스트링으로 사상시키는 함수로 흔히 그 출력을 해쉬값 또는 메시지 다이제스트(message digest)라 한다. 해쉬 함수의 목적은 중요 정보의 전송시 제 3자에 의한 정보의 수정, 삽입 등의 문제에 대해 무결성을 확인하는 것으로 메시지 인증

코드의 구성과 디지털 서명의 효율성 증대를 위해서도 사용된다. 일방향 해쉬 함수는 프리이미지 레지스턴스(preimage resistance)와 세컨드 프리이미지 레지스턴스(second preimage resistance) 성질을 만족해야 하고 암호학적으로 유용한 해쉬 함수는 충돌 회피성(collision resistance)을 만족해야 한다. 즉, 같은 해쉬값을 가지는 서로 다른 두 입력(충돌)을 발견하는 것이 계산상 수행 불가능해야 한다.

해쉬 함수는 크게 블록 암호 알고리즘을 이용한 해쉬 함수와 전용해쉬 함수로 분류한다. DES나 IDEA와 같은 블록 암호를 이용한 경우는 기존의 구현되어 있는 블록 암호를 이용할 수 있다는 장점이 있지만, 블록 암호의 처리 속도가 느리고 수출 제한의 문제로 인해 현재 대부분의 해쉬 함수는 전용 해쉬 함수이다. 전용 해쉬 함수의 대표적인 예로 MD 계열 해쉬 함수가 있다. 기존의 MD 계열 해쉬 함수는 Merkle과 Damgard 의 이론에 기반한 반복적인 처리 형태를 가진다. 1990년에 Rivest에 의해 제안된 MD4 해쉬 함수는 현재 완전히 해독되어 더 이상 안전하지 않고 MD5 역시 내부 취약성이 발견되었다. 1995년 유럽의 RIPE 컨소시움에서 제안한 RIPEMD 역시 안전하지 못한 것으로 증명되었고 다시 이를 개선한 RIPEMD-128/160이 제안된 상태이다. 미국의 NIST에서는 1993년에 SHA를 공개한 후 다시 1995년에 이를 개선한 SHA-1를 발표하였고 현재 미국 표준으로 공인되어 있다. 1993년에 HAVAL 해쉬 함수가 제안되었다. 그 외에 많은 해쉬 함수가 제안되었지만 현재 암호학적으로 안전하다고 간주되는 해쉬 함수로 RIPEMD-160, SHA-1, HAVAL 등이 있다.

그러나, 실제 암호학적으로 안전하고 처리 속도면에서 효율적인 해쉬함수를 구성하는 것은 매우 어려운 문제이다. 해쉬 함수는 임의의 유한 길이 메시지를 고정된 짧은 길이로 사상시키는 함수이기 때문에 같은 해쉬값을 가지는 서로 다른 두 입력 메시지가 항상 존재한다. 따라서 암호학적으로 유용한 해쉬 함수는 이러한 충돌 쌍을 발견하는 것이 계산상 불가능해야 한다. 또한 해쉬 함수는 메시지 인증 코드, 디지털 서명과 같은 다른 응용에 포함되어 사용되어지기 때문에 그 처리 속도가 빨라야 한다.

발명이 이루고자하는 기술적 과제

따라서, 본 발명은 해쉬 함수의 메시지 적용의 단순성을 제거하기 위해 입력 메시지로부터 추가로 메시지를 생성하여 처리하고, 각 단계 연산에 사용되는 부울 함수를 암호학적으로 강한 성질들을 만족하도록 하고, 로테이션(rotation)연산은 입력 메시지에 의존하는 메시지-의존 로테이션(message-dependent rotation)을 사용함으로서 안전성을 향상시키는 해쉬함수를 이용한 정보의 무결성 확인방법을 제공하는데 그 목적이 있다.

상기한 목적을 달성하기 위한 본 발명은 해쉬함수의 각 단계 연산에 있어서, 암호적으로 강한 성질을 만족하는 부울 함수와 입력 메시지에 의존하는 메시지-의존 로테이션(message-dependent rotation)을 사용하는 것을 특징으로 한다.

발명의 구성 및 작용

이하, 첨부도면을 참조하여 본 발명을 상세히 설명하면 다음과 같다.

도 1은 본 발명에 따른 해쉬 함수의 전체적인 구조도이고, 도 2는 본 발명에 따른 압축 함수의 구조도이다.

현재 대부분의 해쉬 함수는 각 메시지 블록에 대해 압축 함수를 반복 적용하는 형태이다. 본 발명은 512 비트 단위로 메시지를 처리하고 160 비트의 연쇄 변수(5개의 워드 A, B, C, D, E)와 160 비트의 해쉬값을 가진다. 워드는 32-비트 크기이다. 처리 과정은 먼저 입력 메시지를 512 비트(16 워드) 블록 단위로 분할하여 처리한다. 입력 메시지가 블록 길이의 배수가 되도록 마지막 블록은 padding을 수행한다. Padding은 마지막 블록 길이가 448비트가 되도록 '1'을 추가한 다음 필요한 수만큼 '0'을 추가한다. 그리고 64비트의 원래 메시지 길이를 추가한다. 각 메시지 블록에 대해 압축 함수를 수행하는데 압축 함수는 4 라운드로 구성된다. 그리고, 압축 함수에서 16개 입력 메시지 블록이 좀더 많은 부분에 사용되도록 추가로 8개의 메시지 블록을 생성한다. 따라서 압축 함수의 각 라운드는 총 24단계로 구성되어 전체 96단계 연산을 수행한다. 메시지 확장은 16개 메시지 워드가 유사한 빈도로 사용되면서 빠르게 구현되도록 하였다.

압축 함수의 각 라운드에 적용되는 메시지 워드의 순서는 추가로 생성된 메시지 워드는 가능한 서로 많이 떨어지도록 하고, 각 단계에서 같은 메시지 워드를 사용하지 않도록 설계되었다. 라운드에서의 단계 연산은 아래 [수학식 1]과 같다.

$$A=(f(A, B, C, D, E) + X_j + K) \lll s, \quad B = B \lll 10$$

연쇄 변수 (A, B, C, D, E)의 초기값 IV는 다음과 같고

A=0x67452301, B=0xefcdab89, C=0x98badcfe, D=0x10325476, E=c3d2e1f0

각 라운드의 단계에 적용되는 상수 K는 다음과 같다.

K_1=0, K_2=0x5a827999, K_3=0x6ed9eba1, K_4=0x8f1bbcdc

각 라운드에서 사용되는 다음의 부울 함수는 0-1 balanced , high nonlinearlity, SAC(Strict Avalanche Criterion)과 같은 암호학적으로 좋은 성질들을 만족한다.

$$f_0(x_1, x_2, x_3, x_4, x_5) = x_1x_2 \oplus x_3x_4 \oplus x_2x_3x_4 \oplus x_5$$

$$f_1(x_1, x_2, x_3, x_4, x_5) = x_2x_3 \oplus x_4x_5 \oplus x_1$$

$f_2(x_1, x_2, x_3, x_4, x_5) = x_1x_3 \cup x_2x_5 \cup x_3x_5 \cup x_4$

그리고, 효율성을 위해 가장 계산량이 적은 부울 함수 f_1을 2 라운드와 4 라운드에서 반복 사용한다. 그리고 단계 연산에서 사용되는 순환이동 s는 입력 메시지에 의존하여 다음처럼 정의된다.

$s=X_i \bmod 32$

여기서의 메시지 워드 X_i는 단계 연산에 적용되는 메시지 워드와 다른 메시지 워드이다.

도 3은 본 발명에 따른 해쉬 함수의 단계 연산의 블록도이고, 도 4는 본 발명에 따른 해쉬 함수에 대한 동작 흐름도이다.

발명의 효과

상술한 바와같이 일반적으로는 중요 정보의 전송시 전송 도중에 발생한 제 3 자에 의한 정보의 수정이나 삽입 등의 문제를 수신측에서 확인할 수 없고, 중요 파일의 저장시에도 타인에 의한 파일의 수정이나 변정 등의 사실을 확인하기 어렵다.

본 발명은 이러한 경우에 전송되는 정보와 함께 그 정보에 대한 해쉬값을 함께 전송함으로서 수신측에서 정보의 무결성을 확인할 수 있고, 파일의 저장시에도 파일에 대한 해쉬값을 유지함으로서 무결성을 확인할 수 있다. 또한 메시지 인증 코드의 구성과 디지털 서명시 그 효율을 향상시키기 위해 본 발명을 사용할 수 있다.

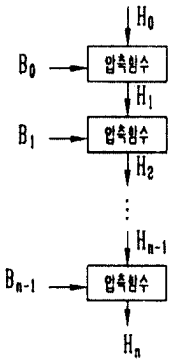
(57) 청구의 범위

청구항 1

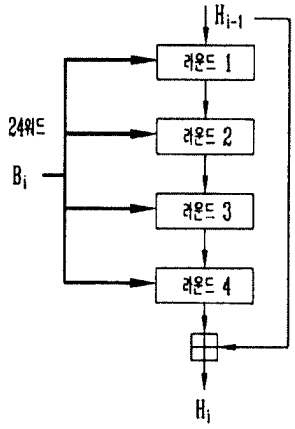
해쉬함수의 각 단계 연상에 있어서, 암호적으로 강한 성질을 만족하는 부울 함수와 입력 메시지에 의존하는 메시지-의존 로테이션(message-dependent rotation)을 사용하는 것을 특징으로 하는 해쉬함수를 이용한 정보의 무결성 확인방법.

도면

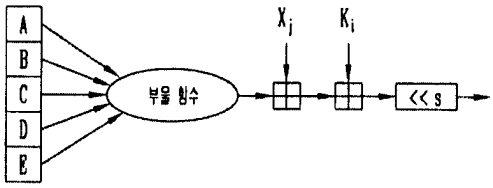
도면1



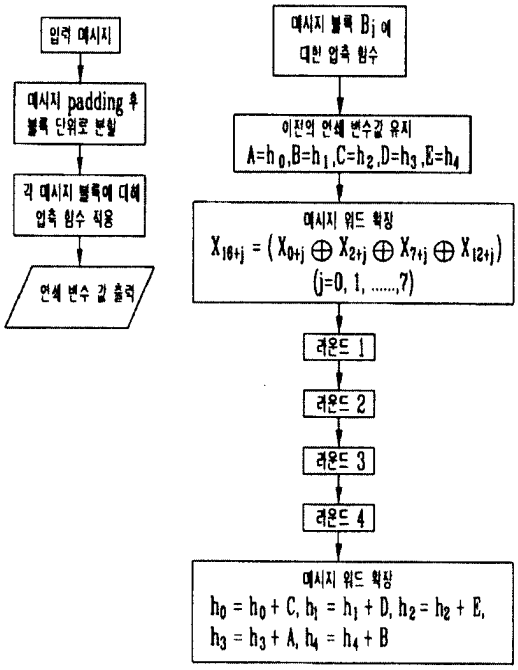
도면2


H_{i-1}
라운드 1
24워드
B_i
라운드 2
라운드 3
라운드 4
H_i

도면3


A
B
C
D
E
부울 함수
X_j
K_i
<< s

도면4


입력 메시지
메시지 padding 후 블록 단위로 분할
각 메시지 블록에 대해 압축 함수 적용
연쇄 변수 값 출력
메시지 블록 B_j 에 대한 압축 함수
이전의 연쇄 변수값 유지
$A=h_0, B=h_1, C=h_2, D=h_3, E=h_4$
메시지 워드 확장
$X_{16+j} = (X_{0+j} \oplus X_{2+j} \oplus X_{7+j} \oplus X_{12+j})$
$(j=0, 1, \ldots\ldots, 7)$
라운드 1
라운드 2
라운드 3
라운드 4
메시지 워드 확장
$h_0 = h_0 + C, h_1 = h_1 + D, h_2 = h_2 + E,$
$h_3 = h_3 + A, h_4 = h_4 + B$